Corr. to JP 20[redacted]-504137

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 12/14

(11) 공개번호 특2000-0049114
(43) 공개일자 2000년07월25일

(21) 출원번호 10-1999-7003195
(22) 출원일자 1999년04월13일
번역문제출일자 1999년04월13일
(86) 국제출원번호 PCT/DE1997/02070 (87) 국제공개번호 WO 1998/16883
(86) 국제출원출원일자 1997년09월15일 (87) 국제공개일자 1998년04월23일
(81) 지정국 EP 유럽특허 : 오스트리아 벨기에 스위스 독일 덴마크 스페인 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투칼 스웨덴 핀랜드
국내특허 : 브라질 중국 일본 대한민국 멕시코 우크라이나 미국 러시아
(30) 우선권주장 19642560.3 1996년10월15일 독일(DE)
(71) 출원인 지멘스 악티엔게젤샤프트 칼 하인쯔 호르닝어
독일 뮌헨 80333 비텔스파허프라쯔 2
(72) 발명자 파프,슈테판
독일데-82049그로쓰헤셀로에베터슈타인슈트라쎄2
(74) 대리인 남상선

심사청구 : 없음

(54) 전자적 데이터 처리 회로

요약

본 발명은 마이크로 프로세서와 같은 오퍼레이팅 모듈, 적어도 하나의 데이터 메모리 및 상기 데이터 메모리와 오퍼레이팅 모듈 사이로 연장하는 데이터 버스를 가지는 전자적 데이터 처리 회로에 관한 것이다.

일반적 타입의 전자적 데이터 처리 회로에서, 상기 메모리는 종종 가능한한 액세싱될 수 없는 정보를 포함한다. 결국, 전자적 데이터 처리 회로의 조작에 대비한 보안 평가를 수행할 필요가 있다.

본 발명의 목적은 원치않는 변경에 대하여 더 나은 보호를 제공하는, 일반적 타입의 전자적 데이터 처리 회로를 제공하는 것이다.

상기 목적은 일반적 타입의 전자적 데이터 처리 회로에 의해 본 발명에 따라 달성되는데, 적어도 하나의 인코딩 모듈(20, 21, 22, 35, 107)이 데이터 메모리(2, 3, 4, 5, 102, 103, 104, 105)와 데이터 버스 사이의 영역 및/또는 오퍼레이팅 모듈(1, 101)과 데이터 버스 사이의 영역에 제공되며, 인코딩 모듈(20, 21, 22, 35, 107)은 오퍼레이팅 모듈(1, 101)과 데이터 버스 사이 또는 데이터 메모리(2, 3, 4, 5, 102, 103, 104, 105)와데이터 버스(106) 사이의 데어터 트래픽이 인코딩 및/또는 디코딩될 수 있도록 설계된다.

대표도

도1

명세서

기술분야

본 발명은 적어도 하나의 데이터 메모리를 가지고 데이터 메모리와 오퍼레이팅 모듈 사이에 연장하는 데이터 버스를 가지는 마이크로 프로세서와 같은 오퍼레이팅 모듈을 구비하는 전자적 데이터 처리 회로에 관한 것이다.

배경기술

일반적 타입의 전자적 데이터 처리 회로는 보안에 관련하여 중요하게 되는 응용에서 빈번히 사용된다. 이런 경우에, 예를 들어 외부 요구때 오퍼레이팅 모듈에 의해 처리되는 기밀 데이터, 머니(money) 값, 액세스 인증은 데이터 메모리에 저장된다.

메모리가 가능한한 액세싱될 수 없는 정보를 포함하기 때문에, 전자적 데이터 처리 회로의 조작에 대한 보안 평가를 수행할 필요가 있다.

일반적 타입의 전자적 데이터 처리 회로가 집적 회로로서 설계될 때, 그것은 서로 다른 패시베이션 층으로 커버될 수 있다. 이런 경우에, 패시베이션 층은 패시베이션 층의 제거가 데이터 메모리의 파괴를 수반하는 식으로 부가될 수 있다. 더욱이, 데이터 메모리는 집적 회로의 더 깊은 하부층내에 매립될 수 있고, 그러므로 그것

에 대한 액세스를 더욱 어렵게 한다.

원치않는 조작으로부터 전자적 데이터 처리 회로를 보호하기 위한 다른 가능성은 전자적 데이터 처리 회로의 동작 조건을 샘플링하는 센서의 사용으로 이루어진다. 센서에 의해 샘플링된 값이 표준값을 벗어나자마자, 적당한 보안 평가가 개시되어 전자적 데이터 처리 회로의 비활성화 또는 데이터 메모리의 소거를 초래한다.

더욱이, 또한 금지 명령 또는 정상 동작 동안 차단되는 어드레스 영역에 대한 액세스 인스턴스를 위해 오퍼레이팅 모듈의 동작으로 모니터링하는 소프트웨어 센서가 있다. 게다가, 액세스 시퀀스가 그것의 정확함을 위해 모니터링될 수 있다.

최종적으로, 인터럽트식으로 구성된 접속 트랙과 같은 특별한 하드웨어 장치에 의해 제한될 수 있는 특별한 제품 모드에서 허용되는, 오퍼레이팅 모듈에 의한 데이터 메모리에 대한 액세스 인스턴스가 추가로 공지되어 있다.

보안 평가가 수행됨에도 불구하고, 원치않는 조작이 일반적 타입의 전자적 데이터 처리 회로에서 때때로 발생한다.

발명의 상세한 설명

본 발명의 목적은 원치않는 변경으로부터 더 양호하게 보호되는 일반적 타입의 전자적 데이터 처리 회로를 제공하는 것이다.

상기 목적은 본 발명에 따른 일반적 타입의 전자적 데이터 처리 회로에 의해 달성되는데, 적어도 하나의 인코딩 모듈이 데이터 메모리와 데이터 버스 사이의 영역 및/또는 오퍼레이팅 모듈과 데이터 버스 사이의 영역에 제공되고, 상기 인코딩 모듈은 오퍼레이팅 모듈과 데이터 버스 사이 또는 데이터 메모리와 데이터 버스 사이의 데이터 트래픽이 인코딩 및/또는 디코딩될 수 있도록 설계된다.

본 발명은 본 발명에 중요한 조사 결과에 기초하는데, 새로운 기술 방법은 집적 회로로서 설계되는 전자적 데이터 처리 회로의 정밀한 조작을 더 용이하게 한다. 그러므로, 조작자의 관점으로부터, 집적 회로내의 전자적 데이터 처리 회로는 전체적으로 칩으로서 뿐만 아니라, 실리콘 기판상의 개별 부품으로 이루어지고 개별적으로 액세싱될 수 있는 부품을 가지는 시스템으로서 간주될 것이다.

따라서 데이터 버스상의 데이터 트래픽을 관찰하거나 또는 데이터 메모리를 판독함으로써 데이터 메모리에 저장된 정보에 대한 판정을 이끌어내는 것이 가능하며, 이것은 조작을 용이하게 한다.

본 발명에 중요한 다른 조사 결과에 따르면, 일반적 타입의 전자적 데이터 처리 회로상의 많은 조작은 성공이 데이터 버스상의 데이터 트래픽 '태핑'으로 얻어진다는 사실에 기인하며, 그 결과로 오퍼레이팅 모듈의 프로그램 흐름이 관찰될 수 있고 바람직하지않은 형태로 이해될 수 있다.

본 발명에 따르면, 전자적 데이터 처리 회로에 인코딩된 데이터를 전송하는 것이 제시되며, 데이터 버스상에 전송된 데이터 트래픽을 인코딩하고 디코딩하기 위해 데이터 버스와 데이터 메모리 사이 또는 오퍼레이팅 모듈과 데이터 버스 사이에 장치들이 제공되어진다. 이런 타입의 장치들은 아래H에서 '인코딩 모듈'로서 표현되고, 이런 표현은 단지 인코딩만을 실행하는 장치에 국한되지 않는다. 본 발명의 기본 사상에 따르면, 이런 표현은 인코딩과 디코딩 둘다 또는 2개 동작중 하나만을 실행하는 장치를 포함한다.

본 발명에 따른 전자적 데이터 처리 회로의 구성은 데이터 버스상에서의 데이터 트래픽의 성공적인 트랙킹의 경우에서도 데이터 메모리에 저장된 데이터상에서 직접 판정을 이끌어 내는 것이 불가능하도록 한다. 더욱이, 데이터 버스상에서 데이터 트래픽을 트랙킹할때 얻어진 정보로부터 프로그램 흐름에 대한 판정을 직접 이끌어내는 것이 불가능하다. 특히, 데이터 메모리에 저장된 데이터가 성공적으로 판독되는 경우에도, 이들이 훈련받지않은 관찰자에게는 무의미하기 때문에 이들의 의미상의 직접 판정을 이끌어내는 것은 불가능하다.

본 발명에 따르면 성공적 조작이 전자적 데이터 처리 회로의 다수의 위치에 대한 동시 관찰을 요구할 것이기 때문에 인코딩과 디코딩이 전체 칩에 걸쳐 방해 또는 혼란되는 형태로 수행된다는 점에서 특히 유리하고, 이것은 단지 기술적 관점으로부터 어렵게 수행될 수 있다.

여기에서 전자적 데이터 처리 회로의 경우에 액세스 인스턴스를 데이터 메모리에 버퍼링하기 위해 인코딩 모듈이 래치 버퍼의 내용이 항상 인코딩되도록 배열되는 래치 버퍼를 제공하는 것이 중요하다. 특히, 래치의 내용은 상대적으로 쉽세 관찰될 수 있고, 그래서 본 발명에 따른 데이터 처리 회로의 동작동안 그것은 보안의 목적을 위해 인코딩된 형태로 제공되어야 한다.

본 발명에 따르면, 인코딩과 디코딩은 가능한한 본 발명에 따른 데이터 처리 회로의 CPU내로 연장될 수 있다. 그러나, 또한 인코딩과 디코딩은 서로 무관하게 다수의 인코딩 모듈에서 수행될 수 있다. 그러나, 본 발명에 따르면 해결책은 단지 단일 인코딩 모듈이 제공되는 것으로 충분하다.

최종적으로, 멀티태스킹 처리로 동시에 서로 다른 응용을 처리하는 데이터 처리 회로의 추가 장점이 있다. 다음에, 서로다른 응용 또는 태스크는 적당한 인코딩에 의해 서로 다른 데이터 메모리에 할당될 수 있고, 서로다른 키가 각각의 태스크에 대해 일치한다. 결과적으로, 어떤 태스크는 다른 태스크의 데이터에 액세싱할 수 없다.

그러므로 본 발명에 따르면 이제 더이상 물리적으로만 데이터 처리 회로를 평가하는 것으로 충분하지않다고 요약될 수 있다. 부가적으로, 특히 다수의 부품를 관찰과 관련하여 인코딩 모듈에 저장된 키, 필요하다면 이런 키의 활성화를 검출하는 것이 필요하다.

본 발명의 실시예에서, 인코딩 모듈은 데이터 버스상의 데이터 트래픽이 인코딩 알고리즘에 의해 인코딩될 수 있도록 설계된다. 인코딩 모듈은 대량 생산에 의해 특히 비용 효율적인 형태로 제조될 수 있는 장점에 의해 수반되는 식으로 설계된다. 그러나, 알고리즘에 의한 인코딩은 그것이 오퍼레이팅 모듈에서의 광범한 계산을 요구하기 때문에 매우 긴 시간이 걸린다. 그러므로 본 발명에 따른 이런 데이터 처리 회로의 실시간 동작은 현재 허용되지않는다.

본 발명의 다른 실시예에서, 인코딩 모듈은 데이터 버스상의 데이터 트래픽이 하드웨어 인코딩에 의해 인코딩될 수 있도록 설계된다. 그것은 엄밀하게 특히 데이터 메모리가 판독을 위해 액세싱될 때 그리고 기록을 위해 액세싱될 때 실시간으로 본 발명에 따른 데이터 처리 회로의 동작을 실현하기에 매우 용이하다.

본 발명에 따르면 하드웨어 인코딩은 데이터 트래픽의 개별 비트의 의미가 선택적으로 변경될 수 있도록 인코딩 모듈에 의해 수행될 수 있다. 다음에 예를 들어 'LOW'로서 메모리에 저장되는 비트가 'HIGH'로서 데이터 버스상의 데이터 트래픽으로 나타난다. 예를 들면, 이것은 적어도 하나의 EXOR 소자를 가지는 인코딩 모듈에 의해 수행된다.

본 발명의 또다른 실시예에서, 인코딩 모듈은 데이터 버스의 데이터 라인의 접속 시퀀스가 선택적으로 변경될 수 있도록 설계된다. 이것은 외부에서 데이터 버스의 개별 비트 라인이 상호변경되는 것처럼 보여진다.

최종적으로, 본 발명에 따른 데이터 처리 회로에서 하드웨어 인코딩은 데이터 버스와 오퍼레이팅 모듈 사이 및/또는 데이터 버스와 데이터 메모리 사이의 데이터 트래픽이 선택적으로, 적어도 부분적으로 지연될 수 있도록 설계되는 인코딩 모듈에 의해 실행될 수 있다. 결과적으로, 데이터 트래픽은 데이터 버스상에서 시뮬레이션되고 본 발명에 따른 전자적 데이터 처리 회로의 순간 동작 상태에 관계없이 유지된다.

본 발명에 따른 데이터 처리 회로의 중요한 특징은 여기에서 인코딩이 선택적으로 동작하도록 인코딩 모듈이 설계되는 것으로 구성된다. 이것은 인코딩이 마음대로 수행되거나 또는 수행되지않는다는 것을 상술한다. 부가적으로, 본 발명에 따르면 이것은 데이터 트래픽을 인코딩하기 위한 서로 다른 키들 사이의 스위칭 가능성을 포함한다. 이런 경우에, 본 발명에 따른 인코딩 모듈의 사용은 다이내믹 작용을 가정한다.

본 발명에 따른 변경 키를 가지는 데이터 처리 회로의 경우에 엄밀하게 배치(batch)로 이루어진 데이터 처리 회로가 각각 서로 다른 개별 키를 가지는 것이 관찰된다. 이것은 어떤 데이터 처리 회로의 키가 공지되어 있더라도 여전히 다른 데이터 처리 회로의 키에 대한 판정을 이끌어낼 수 없다는 것을 보장한다.

본 발명의 기본 사상에 대한 실시예에서, 인코딩 모듈은 적어도 하나의 키를 입력하기 위한 적어도 하나의 입력을 가진다. 그러나, 또한 인코딩 모듈내의 이런 입력은 인코딩 모듈 자체에 저장된 특정 키들사이의 전환 목적을 위해, 그리고 인코딩 모듈에 부가된 인코딩 방법들 사이에도 사용될 수 있다. 또한 전체적으로 간단한 방식으로 단일 인코딩 방법을 활성 또는 비활성화시키는 것이 가능한다. 이런 출발로부터, 또한 입력을 통해 인코딩 모듈 외부에 저장된 키를 입력하는 것이 가능하다. 이런 목적을 위하여, 키는 유리하게 FLASH 셀 또는 EEPROM 셀에 저장된다. 언급된 셀들은 정보가 단지 '약간'의 전자로 플로팅 게이트에 저장되기 때문에 상대적으로 안전한 것으로 간주된다. 이들 내용을 판독하려는 대부분의 방법들은 저장된 정보를 파괴한다. 결국, 본 발명의 실시예에 따르면 데이터 트래픽의 특히 안전한 인코딩이 이루어진다. 더욱이, 모든 FLASH 셀은 프로그래밍가능하다는 장점을 가진다. 그러므로, 본 발명에 따른 데이터 처리 회로를 공급할때 간단한 방법으로 각각의 회로에 개별 키를 프로그램하고 추가 변경을 위해 이들을 차단하는 것이 가능하다.

보안의 추가 개선은 키가 집적 모듈의 매립된 구조에 저장될 때 결과로서 생기고, 집적 모듈은 유리하게 데이터 처리 회로를 수용한다. 매립된 구조는 이들이 집적 모듈내의 서로 다른 위치에서 분산화하여 실행될 수 있는 장점을 제공한다. 이것은 그것이 집적 모듈내에 수용되는 데이터 처리 회로내의 서로 다른 위치에 대해 동시에 관찰될 수 있다는 것이 매우 어렵기 때문에 보안성을 증가시킨다. 더욱이, 또한 키가 저장되는 위치의 조작을 샘플링하고 본 발명에 따른 데이터 처리 회로를 비활성화시키거나 또는 불필요하게 하는 센서를 제공하는 것이 가능하다.

본 발명에 따른 데이터 처리 회로의 제조동안 저장되는 키의 대안으로서, 또한 키가 무작위로 선택될 수 있는 난수 발생기를 제공하는 것이 가능하다.

본 발명의 특히 유리한 실시예에 따르면, 인코딩 모듈에 사용되는 키의 선택은 특히 프로그램 흐름동안 오퍼레이팅 모듈에 의해 수행된다. 이런 목적을 위하여, 본 발명에 따른 데이터 처리 회로는 키가 오퍼레이팅 모듈에 의한 소정 동작의 실행동안 인코딩 모듈내에 입력될 수 있도록 설계된다. 아마 오퍼레이팅 모듈의 프로그램 코드가 공지될 수 있기 때문에, 키를 선택하는 과정은 유리하게 표준 프로그램 코드내에 숨겨진다. 그러므로, 오퍼레이팅 모듈은 예를 들어 CLR C('CLEAR CARRY')와 같은 무익한 명령을 실행하는 경우에 인코딩 모듈의 키가 변경되는 식으로 설계될 수 있다.

그러나, 또한 키의 변화를 모니터링하고 키가 종종 충분히 변경되지않을 때 키의 변화를 개시하는 시간 측정 장치를 제공하는 것이 가능하다.

최종적으로, 인코딩 모듈에 사용된 키와 관련하여 키가 오퍼레이팅 모듈 또는 CPU에 의해 발생된다고 규정되어진다. 예를 들면, 이것은 CPU에 의해 발생된 어드레스로부터 변환 방법에 의해 키를 유도함으로써 수행된다. 이런 방법의 장점은 키가 지속적으로, 다시 말해서 각각의 어드레스로 변경된다는 것이다. 오퍼레이팅 모듈의 프로그래머는 다른 변환 방법을 선택함으로써 인코딩을 좌우할 수 있다.

본 발명에 따른 데이터 처리 회로의 데이터 트래픽은 인코딩 모듈에 사용되는 키가 공지되어진 경우에만 조작자에 의해 이해될 수 있다고 요약될 것이다. 또한 데이터 메모리에 저장된 데이터는 데이터 메모리에 속하는 키의 지식을 가질때만 이해될 수 있다. 이것은 실질적으로 조작에 대비한 보안성을 증진시킨다.

물론, 데이터 처리 회로의 오퍼레이팅 모듈을 프로그래밍하는 프로그래머는 그가 데이터 메모리 또는 데이터 처리 회로의 어드레스에 저장해 놓은 데이터가 키의 일부가 되는 기밀 리스트를 보존하여야 한다. 키의 타입에 의존하여, 프로그래머는 또한 항상 한쌍의 값을 판독할 필요가 있다고 표현되는, 실행될 특정 필수조건을 제공할 수 있다.

전자적 데이터 처리 회로의 특히 유리한 실시예에서, 적어도 2개의 인코딩 모듈이 오퍼레이팅 모듈과 적어도 하나의 데이터 메모리를 접속시키는 데이터 버스의 적어도 하나의 데이터 라인 영역에 제공되며, 상기 인코딩 모듈은 인코딩 또는 디코딩 완료가 2개의 인코딩 모듈의 협동 이외에 의해 수행될 수 없도록 설계된다. 이런 경우에 2개의 인코딩 모듈이 데이터 처리 회로의 서로 다른 위치에 배열되는 것이 유리하다. 이런 실시예는 데이터 트래픽의 인코딩이 2개의 서로 다른 위치에서 수행되는 것을 보장한다. 전형적인 조작자는 아마 특히 단일 인코딩 모듈의 경우에 단일 위치에서 단지 하나의 인코딩을 수행할 것이고, 그럼에도 불구하고 인코딩을

사용할때 유용한 결과에 도달하지 못한다. 엄밀하게 서로 다른 위치에 수용될 수 있는 2개의 인코딩 모듈을 가지는 실시예의 경우에, 미세 구조의 2개의 서로 다른 위치가 특히 어려운 방법으로만 동시에 관찰될 수 있기 때문에 인코팅을 수행하는 것은 특히 어렵다. 그러므로, 상기 구현된 인코딩 모듈은 예를 들어 어떤 인코딩 모듈이 어떤 위치에 있는 데이터 버스의 하위 4개 비트를 인코딩 또는 디코딩하는 동안 다른 인코딩 모듈이 데이터 버스의 나머지 비트를 인코딩 또는 디코딩하는 식으로 구현될 수 있다.

본 발명에 따른 방법의 또다른 장점은 일반적 타입의 데이터 처리 회로의 경우에 데이터 처리 회로의 모든 부품이 서로 통신할 수 없다는 것을 보장하는 보안성 이유가 요구된다는 결과로서 생긴다. 다음에 적당한 키의 구성에 의해, 예를 들어 한정된 수의 인코딩 유니트를 사용하여 상기 목적을 위해 제공되는 데이터 버스의 접속 경로의 경우에만 통신하는 것이 가능하다. 부적당한 인코딩과의 모든 다른 접속은 올바르게 기능할 수 없다.

이제 본 발명에 따른 바람직한 실시예가 첨부된 도면을 참조하여 더욱 상세히 설명될 것이다.

도면의 간단한 설명

도 1은 CPU에 단지 하나의 인코딩 장치를 가지는 본 발명에 따른 전자적 데이터 처리 회로를 도시하고,

도 2는 도 1의 전자적 데이터 처리 회로의 변형예이며,

도 3은 CPU와 데이터 메모리 영역에 인코딩 장치를 가지는 본 발명에 따른 다른 전자적 데이터 처리 회로를 도시한다.

실시예

도 1은 본 발명에 따른 데이터 처리 회로를 도시하는데, 상기 회로는 오퍼레이팅 모듈로서 CPU(101)와 다수의 데이터 메모리를 가진다. 상세히, 이것들은 ROM(102), EEPROM(103), FLASH 메모리(104) 및 RAM(105)이다. 상기 데이터 메모리(102, 102, 104, 105)와 CPU(101)는 서로 데이터 버스(106)를 통해 접속된다.

상기 CPU(101)에 제공된 것은 CPU(101)와 데이터 메모리(102, 103, 104 및 105) 사이의 데이터 트래픽을 인코딩 또는 디코딩하는 인코딩 모듈(107)이다. 여기에서 이런 타입의 장치가 단지 인코딩을 수행하는 장치에 국한되지않더라도 아래에 '인코딩 모듈'로서 참조된다는 것이 다시 한번 언급될 수 있다. 본 발명의 기본 사상에 따르면, 또한 이런 지정은 인코딩과 디코딩 둘다 또는 2가지 동작중 하나만을 수행하는 장치를 포함한다. 상기 인코딩 또는 디코딩은 이런 경우에 적당한 지연에 의해, 데이터 버스의 개별 비트 라인의 교환에 의해, 또는 개별 데이터 비트의 의미를 변경함으로써 수행될 수 있다. 또한 소프트웨어 인코딩을 수행하는 것이 가능하다.

더욱이, 본 발명에 따른 데이터 처리 회로는 데이터 라인(109)을 통해 FLASH 메모리(104)에 접속되는 멀티플렉서(108)를 가진다. 상기 멀티플렉서(108)는 데이터 라인(110)을 통해 타이머(111)에 접속되는데, 상기 타이머(111)에는 데이터 라인(112)을 통해 난수 발생기(113)에 의한 난수가 공급될 수 있다. 또한 상기 멀티플렉서(108)는 ROM(102)에 접속되는 제어 라인(114)을 가진다. 최종적으로, 또한 규정이 멀티플렉서(108)에 대해 리셋 라인(115)으로 형성되고, 그것을 통해 멀티플렉서(108)는 데이터 처리 회로의 리셋의 경우에 개시 상태로 리셋될 수 있다. 상기 멀티플렉서(108)의 출력은 제어 라인(116)을 통해 인코딩 모듈(107)에 접속되고, 상기 인코딩 모듈(107)은 멀티플렉서(108)의 출력 신호에 응답하여 새로운 키를 공급받는다. 본 발명에 따르면, 또한 인코딩 모듈(107)에 사용된 인코딩 방법이 제어 라인(116)을 통해 멀티플렉서(108)의 출력 신호에 응답하여 인코딩 모듈(107)로 전환된다고 규정되어 있다.

동작중, 본 발명에 따른 전자적 데이터 처리 회로는 다음과 같이 동작한다. 프로그램이 시작(리셋될 때), 시작키는 리셋 라인(115)상의 신호에 응답하여 멀티플렉서에 놓인다. 그때, 데이터 버스(106)와 CPU(101) 사이의 데이터 트래픽은 인코딩 모듈(107)에서 인코딩 또는 디코딩되고, 상응하는 동작이 데이터 흐름 방향에 따라 인코딩 모듈(107)을 통한 각각의 데이터 경로상에서 실행된다. 명령 'CLR C'의 실행으로, 상기 ROM(102)은 제어 라인(114)을 통해 멀티플렉서(108)에 제어 펄스를 전송한다. 그결과, 상기 멀티플렉서(108)는 데이터 라인(109)을 통해 FLASH 메모리(104)로부터 3개의 키(키 3, 키 2, 키 1)중 하나를 추출하며, 그것을 인코딩 모듈(107)로 전송한다. 그후, 인코딩 모듈(107)에 사용된 키가 교환되거나, 제어 라인(116)에 제공되는 신호의 의미에 의존하여 인코딩 모듈(107)에 사용된 인코딩 방법으로부터의 변형이 주어진다. 데이터 처리 회로의 특정 동작 시간이 멀티플렉서(108)가 ROM(102)에 의해 활성화되지않고 초과한다면, 상기 타이머(111)가 동작하게 된다. 상기 타이머(111)의 활성화는 난수 발생기(113)로부터의 난수를 데이터 라인(110)을 통해 멀티플렉서(108)로 전송한다. 다음에 상기 멀티플렉서(108)는 난수를 인코딩 모듈(107)로 전송한다.

상기 데이터 메모리(102, 103, 104 및 105)내의 데이터는 인코딩된 형태로 저장된다. 결국, 상기 데이터 버스(106)상의 데이터는 인코딩된 형태로 CPU(101)로 전송되고, 여기에서 이들은 다시 인코딩 모듈(107)에 의해 디코딩된다. 그후에만 데이터는 CPU에서의 처리를 위해 디코딩될 준비를 한다.

도 2는 마찬가지로 오퍼레이팅 모듈로서 CPU(101)를 가지고 뿐만 아니라 다수의 메모리를 가지는, 도 1의 데이터 처리 회로의 변형예를 도시한다. 상세히, 이런 것은 OM9102), EEPROM(103), FLASH 메모리(104) 및 RAM(105)이다. 상기 데이터 메모리(102, 103, 104, 105)와 CPU(101)는 서로 데이터 버스(106)를 통해 접속된다.

상기 CPU(101)에 제공된 것은 CPU(101)와 데이터 메모리(102, 103, 104 및 105) 사이의 데이터 트래픽을 인코딩 또는 디코딩하는 인코딩 모듈(107)이다.

도1과 대조적으로, 도 2의 데이터 처리 회로는 인코딩 모듈(107)에 새로운 키를 공급하는 멀티플렉서가 없다. 이것 대신에, 도 2의 데이터 처리 회로는 제어 라인(122)을 통해 부분적으로 CPU(101)의 어드레스 버스(121)에 접속되는 변환 모듈(120)에 접속된다. 상기 변환 모듈(120) 이외에 특정 변환이 '어드레스'로부터 '키'로 변환 모듈(102)에 저장되는 서로다른 변환의 선택으로부터 선택될 수 있는 추가 제어 라인(123)이 제공된다. 그

결과 키가 변환 모듈(120)에 의해 CPU(101)에 존재하는 어드레스로부터 유도된다.

동작중, 도 2의 전자적 데이터 처리 회로는 본질적으로 도 1의 그것과 같이 동작한다. 프로그램이 시작(리셋)될 때, 시작 키가 제어 라인(123)상의 신호에 응답하여 인코딩 모듈(107)에 놓인다. 그후, 데이터 버스(106)와 CPU(101) 사이의 각각의 데이터 트래픽 인스턴스는 인코딩 모듈(107)에서 인코딩 또는 디코딩되고, 상응하는 동작이 인코딩 모듈(107)을 통과하는 데이터 경로에서 데이터 흐름 방향으로 실행된다. 제어 라인(123)의 각각의 활성화로, 상기 변환 모듈(120)은 새로운 변환에 기초하여 CPU(101)에 존재하는 어드레스로부터 키를 유도한다.

상기 데이터 메모리(102, 103, 104 및 105)내의 데이터는 항상 인코딩된 형태로 저장된다. 결국, 데이터 버스(106)상의 데이터는 인코딩된 형태로 CPU(01)로 전송되고, 여기에서 이들은 다시 인코딩 모듈(107)에 의해 인코딩된다. 그후에만 데이터는 CPU에서의 처리를 위해 디코딩될 준비를 한다.

도 3의 본 발명에 따른 데이터 처리 회로는 오퍼레이팅 모듈로서의 CPU(1) 및 다수의 데이터 메모리를 가진다. 상세히, 이것들은 ROM(2), EEPROM(3), FLASH 메모리(4) 및 RAM(5)이다. 상기 데이터 메모리(2, 3, 4, 5)와 CPU(1)는 데이터 버스(도시안됨)를 통해 서로 접속된다. 상기 데이터 버스 대신에, 개별 데이터 라인(6, 7, 8, 9, 10, 11, 12, 13, 14 및 15)가 제공되는데, 그것을 통해 CPU(1)는 데이터 메모리(2, 3, 4, 5)와 데이터를 교환한다. 어떤 래치 버퍼(16, 17, 18, 19)가 CPU(1)와 ROM(2), EEPROM(3), FLASH(4) 그리고 RAM(5) 사이에 각각 추가로 배열된다.

ROM(2)과 래치(6) 사이의 영역, 래치(17)와 CPU(1) 사이의 영역, 래치들(18, 19)과 CPU(1) 사이의 영역, 및 CPU(1) 자체의 영역에 제공된 것은 인코딩 모듈(20, 21, 22 및 35)인데, 상기 인코딩 모듈은 그들에 할당된 데이터 라인상의 데이터 트래픽을 인코딩 또는 디코딩한다. 여기에서 이런 타입의 장치가 단지 인코딩을 수행하는 장치에 국한되지않더라도 아래에 '인코딩 모듈'로서 참조된다는 것이 다시 한번 언급될 수 있다. 본 발명의 기본 사상에 따르면, 또한 이런 지정은 인코딩과 디코딩 둘다 또는 2가지 동작중 하나만을 수행하는 장치를 포함한다. 상기 인코딩 또는 디코딩은 이런 경우에 적당한 지연에 의해, 데이터 버스의 개별 비트 라인의 교환에 의해, 또는 개별 데이터 비트의 의미를 변경함으로써 수행될 수 있다. 또한 소프트웨어 인코딩을 수행하는 것이 가능하다.

상기 인코딩 모듈(20 21, 22 및 35)은 그들에 할당된 데이터 라인상의 데이터 트래픽이 부분적으로만 인코딩 또는 디코딩되도록 설계된다. 완전한 인코딩 또는 디코딩은 인코딩 모듈(35)과 인코딩 모듈(20, 21, 22)중 하나와의 협동에 의해서만 얻어진다.

더욱이, 본 발명에 따른 데이터 처리 회로는 데이터 라인(24)를 통해 FLASH 메모리(4)에 접속되는 멀티플렉서(23)를 가진다. 상기 멀티플렉서(23)는 데이터 라인(25)을 통해 타이머(26)에 접속되고, 상기 타이머(26)에는 데이터 라인(27)을 통해 난수 발생기(28)에 의한 난수가 공급된다. 또한 상기 멀티플렉서(28)는 그것이 ROM(2)에 접속되는 제어 라인(29)을 가진다.

상기 멀티플렉서(23)의 출력은 제어 라인(30, 31, 32, 33, 34)을 통해 인코딩 모듈(20, 21, 22, 35)에 접속되고, 상기 인코딩 모듈(20, 21, 22, 35)에는 멀티플렉서(23)에 응답하여 새로운 키가 공급된다.

동작중, 본 발명에 따른 전자적 데이터 처리 회로는 다음과 같이 동작한다. 명령 'CLR C'의 실행으로, 상기 ROM(2)은 제어 라인(29)을 통해 제어 펄스를 멀티플렉서(23)로 전송한다. 그결과, 상기 멀티플렉서(23)는 데이터 라인(24)을 통해 FLASH 메모리(4)로부터 3개의 키(키 3, 키 2, 키 1)중 하나를 추출하며, 그것을 인코딩 모듈(20, 21, 22 및 35)로 전송한다. 데이터 처리 회로의 소정 동작 시간이 멀티플렉서(23)가 ROM(2)에 의해 활성화되지않고 초과한다면, 상기 타이머(26)가 동작하게 된다. 상기 타이머(26)의 활성화는 난수 발생기(28)로부터의 난수를 데이터 라인(25)을 통해 멀티플렉서(23)로 전송한다. 다음에 상기 멀티플렉서(23)는 난수를 인코딩 모듈(20, 21, 22, 35)로 전송한다.

상기 ROM(2)내의 데이터는 인코딩된 형태로 저장되고, 이들은 래치(16)에서의 판독동안 인코딩 장치(20)에 의해 부분적으로만 디코딩된다. 결국, ROM(2)으로부터의 데이터는 데이터 라인(8)상에서 여전히 부분적으로 인코딩되어 CPU(1)까지 전송되고, 여기에서 이들은 인코딩 모듈(35)에 의해 완전히 디코딩된다. 그후에만 데이터는 CPU(1)에서의 처리를 위해 디코딩될 준비를 한다.

EEPROM(3)에 인코딩된 형태로 제공되는 데이터는 인코딩되어 데이터 라인(9)을 통해 래치(17)로 전송되며, 거기로부터 인코딩 모듈(21)로 교대하여 보내지고, 여기에서 이들은 부분적으로 디코딩된다. 거기로부터, 여전히 부분적으로 인코딩된 데이터는 데이터 라인(11)을 통해 CPU(1)로 전달되고, 여기에서 이들은 인코딩 모듈(35)에 의해 완전히 디코딩되어 그후 처리를 위해 이용된다.

FLASH 메모리(4)와 RAM(5)을 위한 데이터는 이들이 완전히 인코딩되어 FLASH 메모리(4) 또는 RAM(5)에 저장되기 이전에 초기에 각각 인코딩 모듈(35)과 인코딩 모듈(22)에 의해 부분적으로 인코딩된다. 이런 목적을 위해, CPU(1)의 인코딩 모듈(35)에서 부분적으로 인코딩된 데이터는 데이터 라인(11)을 통해 인코딩 모듈(22)로 전송되고, 여기에서 이들이 데이터 라인(13과 14)을 통해 FLASH 메모리(4)와 RAM(5)에 할당된 래치(18, 19)에 전달되기 이전에 이들은 완전히 인코딩된다. 상기 인코딩된 데이터는 데이터 라인(12, 15)을 통해 래치(18, 19)로부터 FLASH 메모리(4) 또는 RAM(5)으로 전달된다.

데이터가 FLASH 메모리(4)와 RAM(5)에서 판독될 때, 이들이 CPU(1)에서 완전히 디코딩되어 처리에 이용되기 이전에 이들은 처음에 각각 인코딩 모듈(22)과 인코딩 모듈(35)에 의해 부분적으로 디코딩된다.

(57) 청구의 범위

청구항 1

마이크로 프로세서와 같은 오퍼레이팅 모듈, 적어도 하나의 데이터 메모리 및 상기 데이터 메모리와 오퍼레이팅 모듈 사이로 연장하는 데이터 버스를 가지는 전자적 데이터 처리 회로에 있어서,

적어도 하나의 인코딩 모듈(20, 21, 22, 35, 107)이 상기 데이터 메모리(2, 3, 4, 5, 102, 103, 104, 105)와 데이

터 버스(106) 사이의 영역 및/또는 상기 오퍼레이팅 모듈(1, 101)과 데이터 버스(106) 사이의 영역에 제공되며, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 상기 오퍼레이팅 모듈(1, 101)과 데이터 버스(106) 사이 또는 상기 데이터 메모리(2, 3, 4, 5, 102, 103, 104, 105)와 데이터 버스(106) 사이의 데이터 트래픽이 인코딩 및/또는 디코딩 될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 2

제 1항에 있어서, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 상기 데이터 트래픽이 인코딩 알고리즘에 의해 인코딩될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 3

제 1항 또는 제 2항에 있어서, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 상기 데이터 트래픽이 하드웨어 인코딩에 의해 인코딩될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 4

제 3항에 있어서, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 상기 데이터 트래픽의 개별 비트 의미가 선택적으로 변경될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 5

제 4항에 있어서, 상기 인코딩 모듈은 적어도 하나의 EXOR 소자를 가지는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 6

제 3항 내지 제 5항중 어느 한항에 있어서, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 상기 데이터 버스의 데이터 라인의 접속 시퀀스가 선택적으로 변경될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 7

제 3항 내지 제 6항중 어느 한항에 있어서, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 상기 데이터 트래픽이 적어도 부분적으로, 선택적으로 지연될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 8

제 3항 내지 제 7항중 어느 한항에 있어서, 상기 인코딩 모듈(20, 21, 22, 35, 107)은 적어도 하나의 키를 입력하기 위한 적어도 하나의 입력부를 가지는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 9

제 8항에 있어서, 상기 키는 상기 데이터 처리 회로의 플래시 셀에 저장되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 10

제 7항 또는 제 8항에 있어서, 상기 키는 상기 데이터 처리 회로를 수용하기 위한 집적 모듈의 매립된 구조물에 저장되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 11

제 8항 또는 제 9항에 있어서, 상기 키가 저장되는 위치의 조작을 샘플링 하기 위해 센서 기술을 사용하는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 12

제 8항 내지 제 11항중 어느 한항에 있어서, 상기 데이터 처리 회로는 상기 오퍼레이팅 모듈에 의한 소정 동작의 실행동안 어떤 키가 상기 인코딩 모듈(20, 21, 22, 35, 107)내에 입력될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 13

제 8항 내지 제 12항중 어느 한항에 있어서, 어떤 키가 무작위로 선택될 수 있는 난수 발생기(28)가 제공되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 14

제 8항 내지 제 12항중 어느 한항에 있어서, 상기 오퍼레이팅 모듈(101)에 사용된 어드레스로부터 어떤 키를 유도하기 위한 장치가 제공되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 15

제 8항 내지 제 13항중 어느 한항에 있어서, 어떤 키의 변화가 개시될 수 있도록 하는 시간 측정 장치(26)가 제공되는 것을 특징으로 하는 전자적 데이터 처리 회로.

청구항 16

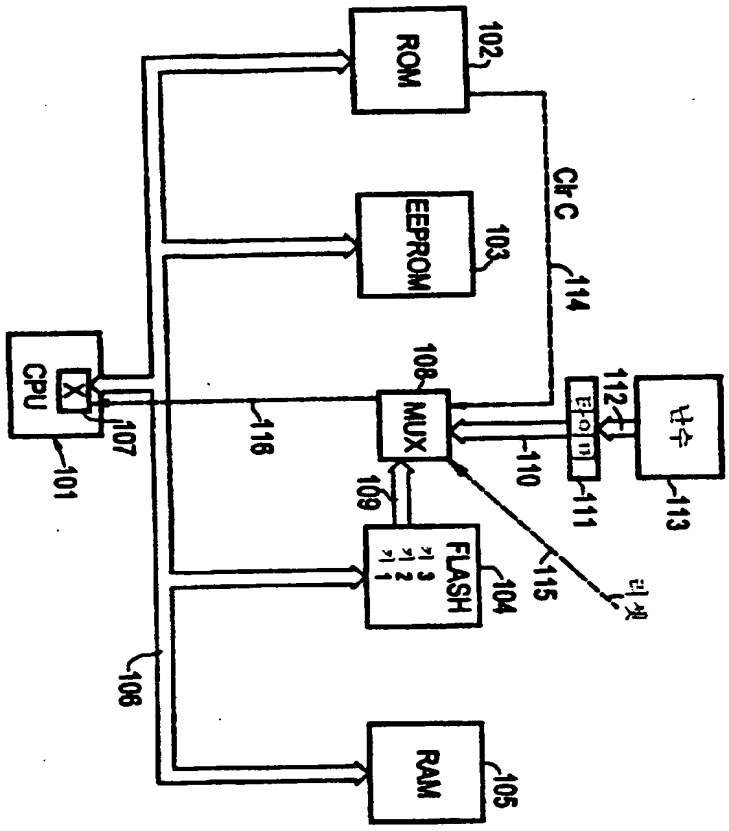
전술한 항중 어느 한항에 있어서, 적어도 2개의 인코딩 모듈(18, 19, 20, 21, 35)이 상기 데이터 버스의 적어도 하나의 데이터 라인(7, 8, 34, 11) 영역에 제공되는데, 상기 데이터 라인은 오퍼레이팅 모듈(1)과 적어도 하나

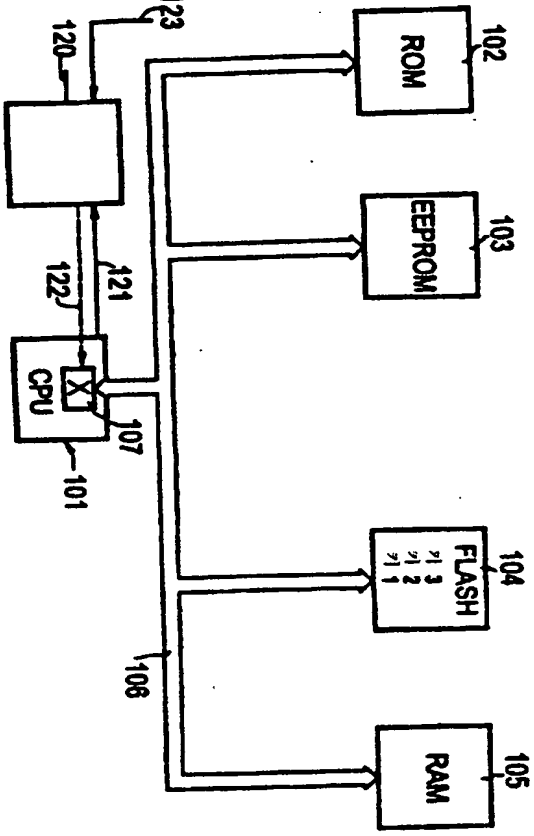
의 데이터 메모리(2, 3, 4, 5)를 접속시키며, 상기 인코딩 모듈(18, 19, 20, 21, 35)는 완전한 인코딩 또는 디코딩이 상기 인코딩 모듈(18, 19, 20, 21, 35)의 협동에 의해 실행될 수 있도록 설계되는 것을 특징으로 하는 전자적 데이터 처리 회로.

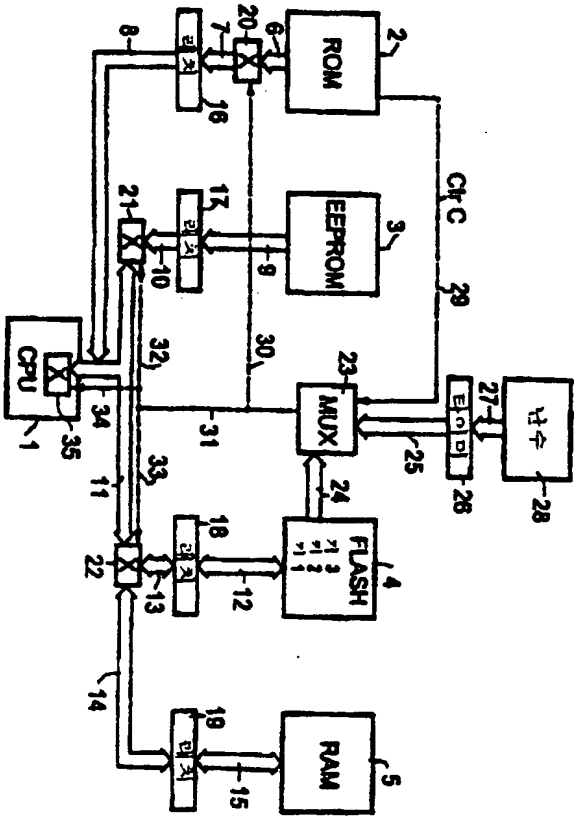
청구항 17

제 16항에 있어서, 상기 인코딩 모듈(18, 19, 20, 21, 35)은 상기 전자적 데이터 처리 회로의 서로 다른 위치에 배치되는 것을 특징으로 하는 전자적 데이터 처리 회로.

도면




ROM
102
EEPROM
103
FLASH
104
RAM
105
CPU
101
120
121
122
123
106
107


ROM
2
EEPROM
3
FLASH
4
RAM
5
CPU
1
MUX
23
CtrC
29
29
28
27
25
24
30
31
32
33
34
35
11
22
14
6
7
8
9
10
12
13
15
16
17
18
19
20
21